

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-142702

(43)Date of publication of application : 02.06.2005

(51)Int.Cl.

H04L 12/66

H04L 12/46

H04L 12/56

(21)Application number : 2003-375352

(71)Applicant : NEC CORP

(22)Date of filing : 05.11.2003

(72)Inventor : FUJITA NORITO
ISHIKAWA YUICHI
IWATA ATSUSHI

(54) NETWORK ACCESS GATEWAY, NETWORK ACCESS GATEWAY CONTROL METHOD, AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable each terminal in a LAN accommodated in the network access gateway to access an optional number of target networks (target VLAN) at the same time.

SOLUTION: When receiving an authentication request particularizing a target VLAN (e.g. target VLAN D1, D3) desirably accessed from a terminal A1 in the LAN, a terminal authentication section B11 in the network access gateway B1 authenticates whether or not the access to the target VLAN D1, D3 is possible. When accessible, a session management section B12 generates a virtual interface to an interface driver B17 so that the access from the terminal A1 to the target VLAN D1, D3 is possible and makes settings for transfer of packets transmitted from / received by the terminal A1 to a routing table B13 and further settings for transfer of a DNS query transmitted from the terminal A1 to a DNS query transfer table B15.



LEGAL STATUS

[Date of request for examination]

05.11.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-142702

(P2005-142702A)

(43) 公開日 平成17年6月2日(2005.6.2)

(51) Int.Cl. ⁷	F I	テーマコード (参考)
HO4L 12/66	HO4L 12/66	5K030
HO4L 12/46	HO4L 12/46	5K033
HO4L 12/56	HO4L 12/56	H

審査請求 有 請求項の数 39 O L (全 37 頁)

(21) 出願番号	特願2003-375352 (P2003-375352)	(71) 出願人	000004237
(22) 出願日	平成15年11月5日 (2003.11.5)		日本電気株式会社
		(74) 代理人	100088959
			弁理士 境 廣巳
		(72) 発明者	藤田 範人
			東京都港区芝五丁目7番1号 日本電気株
			式会社内
		(72) 発明者	石川 雄一
			東京都港区芝五丁目7番1号 日本電気株
			式会社内
		(72) 発明者	岩田 淳
			東京都港区芝五丁目7番1号 日本電気株
			式会社内

最終頁に続く

(54) 【発明の名称】 ネットワークアクセスゲートウェイ及びネットワークアクセスゲートウェイの制御方法並びにプログラム

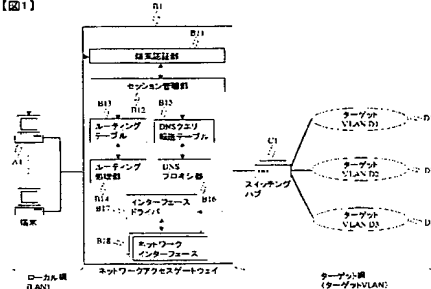
(57) 【要約】

【課題】 ネットワークアクセスゲートウェイに收容されるLAN内の各端末が、それぞれ任意の数のターゲット網（ターゲットVLAN）に同時にアクセスできるようにする。

【解決手段】 ネットワークアクセスゲートウェイB1内の端末認証部B11は、LAN内の端末A1からアクセスしたいターゲットVLAN（例えば、ターゲットVLAN D1, D3）を特定した認証要求が送られてくると、ターゲットVLAN D1, D3に対するアクセスが可能か否かを認証する。アクセス可能な場合、セッション管理部B12は、端末A1からターゲットVLAN D1, D3へのアクセスが可能になるように、インターフェースドライバB17に対して仮想インターフェースを作成すると共に、端末A1が送受信するパケットを転送するための設定をルーティングテーブルB13に対して行い、さらに端末A1が送信するDNSクエリを転送するための設定をDNSクエリ転送テーブルB15に対して行う。

【選択図】 図1

【図1】



【特許請求の範囲】**【請求項 1】**

L A Nと該L A N内のノードからのアクセスの候補となる複数のターゲット網を含むW A Nとの境界に設置され、前記L A N内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、

前記ノードごとに、1つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えることを特徴とするネットワークアクセスゲートウェイ。

【請求項 2】

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする請求項 1 に記載のネットワークアクセスゲートウェイ。

10

【請求項 3】

L A Nと該L A N内のノードからのアクセスの候補となる複数のターゲット網を含むW A Nとの境界に設置され、前記L A N内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部と、

該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部とを備えること

を特徴とするネットワークアクセスゲートウェイ。

20

【請求項 4】

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする請求項 3 に記載のネットワークアクセスゲートウェイ。

【請求項 5】

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第 1 のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第 2 のエントリが格納される名前解決クエリ転送テーブルとを備え、

30

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記ルーティングテーブルに対して第 1 のエントリを作成し、前記名前解決クエリ転送テーブルに対して第 2 のエントリを作成すること

を特徴とする請求項 3 または 4 のいずれかに記載のネットワークアクセスゲートウェイ。

【請求項 6】

前記名前解決クエリは D N S クエリであり、前記名前解決クエリ転送テーブルは D N S クエリ転送テーブルであること

40

を特徴とする請求項 5 に記載のネットワークアクセスゲートウェイ。

【請求項 7】

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする請求項 3 乃至 6 のいずれかに記載のネットワークアクセスゲートウェイ。

【請求項 8】

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有す

50

る認証VLANスイッチに問い合わせることにより認証を行うこと
を特徴とする請求項3乃至6のいずれかに記載のネットワークアクセスゲートウェイ。

【請求項9】

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントを有すること

を特徴とする請求項3乃至8のいずれかに記載のネットワークアクセスゲートウェイ。

【請求項10】

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられること

を特徴とする請求項3乃至9のいずれかに記載のネットワークアクセスゲートウェイ。

【請求項11】

複数の前記ターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求める機能を有するIPアドレス領域重複検出部を備えること

を特徴とする請求項3乃至10のいずれかに記載のネットワークアクセスゲートウェイ。

【請求項12】

前記セッション管理部は、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記IPアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第3のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するIPアドレス領域を互いに重複しないIPアドレス領域にIPアドレス変換するように第1のエントリおよび第3のエントリを設定すること
を特徴とする請求項11に記載のネットワークアクセスゲートウェイ。

【請求項13】

前記名前解決クエリはDNSクエリであり、前記名前解決応答はDNS応答であり、前記名前解決クエリ／応答転送テーブルはDNSクエリ／応答転送テーブルであること

を特徴とする請求項12に記載のネットワークアクセスゲートウェイ。

【請求項14】

LANと該LAN内のノードからのアクセスの候補となる複数のターゲット網を含むWANとの境界に設置され、前記LAN内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、

前記ノードごとに、1つまたは複数の前記ターゲット網へのアクセスのための環境設定を行うことを特徴とするネットワークアクセスゲートウェイの制御方法。

【請求項15】

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする請求項14に記載のネットワークアクセスゲートウェイの制御方法。

【請求項16】

LANと該LAN内のノードからのアクセスの候補となる複数のターゲット網を含むWANとの境界に設置され、前記LAN内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、

10

20

30

40

50

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証ステップと、

該端末認証ステップで認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理ステップとを含むことを特徴とするネットワークアクセスゲートウェイの制御方法。

【請求項 17】

前記セッション管理ステップは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする請求項 16 に記載のネットワークアクセスゲートウェイの制御方法。

10

【請求項 18】

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第 1 のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第 2 のエントリが格納される名前解決クエリ転送テーブルとを備え、

前記セッション管理ステップでは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記ルーティングテーブルに対して第 1 のエントリを作成し、前記名前解決クエリ転送テーブルに対して第 2 のエントリを作成することを特徴とする請求項 16 または 17 のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

20

【請求項 19】

前記名前解決クエリは DNS クエリであり、前記名前解決クエリ転送テーブルは DNS クエリ転送テーブルであること

を特徴とする請求項 18 に記載のネットワークアクセスゲートウェイの制御方法。

【請求項 20】

前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする請求項 16 乃至 19 のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

30

【請求項 21】

前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証 VLAN スイッチに問い合わせることにより認証を行うことを特徴とする請求項 16 乃至 19 のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

40

【請求項 22】

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得するパラメータ取得ステップを含むこと

を特徴とする請求項 16 乃至 21 のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

【請求項 23】

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられること

50

を特徴とする請求項 16 乃至 22 のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

【請求項 24】

複数の前記ターゲット網の各々で利用されている IP アドレスの領域が重複するかどうかを調べ、重複があった場合は、重複する IP アドレス領域をどのように IP アドレス変換すべきかを求める機能を有する IP アドレス領域重複検出ステップを含むことを特徴とする請求項 16 乃至 23 のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

【請求項 25】

前記セッション管理ステップでは、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記 IP アドレス領域重複検出ステップを介して、前記複数のターゲット網の各々で利用されている IP アドレスの領域が重複するかどうかを調べ、重複があった場合は、重複する IP アドレス領域をどのように IP アドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第 1 のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第 3 のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複する IP アドレス領域を互いに重複しない IP アドレス領域に IP アドレス変換するように第 1 のエントリおよび第 3 のエントリを設定することを特徴とする請求項 24 に記載のネットワークアクセスゲートウェイの制御方法。

【請求項 26】

前記名前解決クエリは DNS クエリであり、前記名前解決応答は DNS 応答であり、前記名前解決クエリ／応答転送テーブルは DNS クエリ／応答転送テーブルであること
を特徴とする請求項 25 に記載のネットワークアクセスゲートウェイの制御方法。

【請求項 27】

コンピュータを、LAN と該 LAN 内のノードからのアクセスの候補となる複数のターゲット網を含む WAN との境界に設置され、前記 LAN 内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、前記ノードごとに、1 つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えるネットワークアクセスゲートウェイとして機能させるためのプログラム。

【請求項 28】

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする請求項 27 に記載のプログラム。

【請求項 29】

コンピュータを、LAN と該 LAN 内のノードからのアクセスの候補となる複数のターゲット網を含む WAN との境界に設置され、前記 LAN 内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部、

該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部として機能させるためのプログラム。

【請求項 30】

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための

10

20

30

40

50

環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする請求項 29 に記載のプログラム。

【請求項 31】

前記コンピュータが、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第 1 のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第 2 のエントリが格納される名前解決クエリ転送テーブルとを備え、

10

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記ルーティングテーブルに対して第 1 のエントリを作成し、前記名前解決クエリ転送テーブルに対して第 2 のエントリを作成すること

を特徴とする請求項 29 または 30 のいずれかに記載のプログラム。

【請求項 32】

前記名前解決クエリは DNS クエリであり、前記名前解決クエリ転送テーブルは DNS クエリ転送テーブルであること

を特徴とする請求項 31 に記載のプログラム。

20

【請求項 33】

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする請求項 29 乃至 32 のいずれかに記載のプログラム。

【請求項 34】

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証 VLAN スイッチに問い合わせることにより認証を行うこと

を特徴とする請求項 29 乃至 32 のいずれかに記載のプログラム。

30

【請求項 35】

前記コンピュータを、

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントとして機能させること

を特徴とする請求項 29 乃至 34 のいずれかに記載のプログラム。

【請求項 36】

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられること

を特徴とする請求項 29 乃至 35 のいずれかに記載のプログラム。

40

【請求項 37】

前記コンピュータを、

複数の前記ターゲット網の各々で利用されている IP アドレスの領域が重複するかどうかを調べ、重複があった場合は、重複する IP アドレス領域をどのように IP アドレス変換すべきかを求める IP アドレス領域重複検出部として機能させること

を特徴とする請求項 29 乃至 36 のいずれかに記載のプログラム。

【請求項 38】

前記セッション管理部は、

50

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記IPアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第3のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するIPアドレス領域を互いに重複しないIPアドレス領域にIPアドレス変換するように第1のエントリおよび第3のエントリを設定すること

を特徴とする請求項37に記載のプログラム。

【請求項39】

前記名前解決クエリはDNSクエリであり、前記名前解決応答はDNS応答であり、前記名前解決クエリ／応答転送テーブルはDNSクエリ／応答転送テーブルであること
を特徴とする請求項38に記載のプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワークアクセスゲートウェイに関し、特に、LAN(Local Area Network)内のノードとWAN(Wide Area Network)との境界に設置され、LAN内のノードをWANに接続させるネットワークアクセスゲートウェイに関する。

【背景技術】

【0002】

従来からLAN内のノードとWANとの境界に設置され、LAN内のノードをWANに接続させるためのネットワークアクセスゲートウェイとしては種々のものが知られている（例えば、特許文献1参照）。このようなネットワークアクセスゲートウェイの利用例としては、家庭やオフィスからインターネットや企業基幹網にアクセスするためのアクセスゲートウェイとしての利用が挙げられる。また他にも、網事業者における利用も考えられ、ホットスポット、マンション、オフィスビルディング等における加入者ノードの集線装置としての利用が挙げられる。網事業者における利用の場合は、加入者認証機能や課金機能など、家庭やオフィスにおける利用の場合よりも高度な機能が要求される。

【0003】

この種のネットワークアクセスゲートウェイは、LAN内の複数のノードを収容することができる。LAN内のノードに対しては、自ゲートウェイがDHCP(Dynamic Host Configuration Protocol)サーバとなって動的にIPアドレスを払い出し、自動的にノードの設定を行うことも可能である。このとき払い出すIPアドレスとしては、グローバルIPアドレス空間との重複を避けるためにプライベートIPアドレスが主に用いられる。

【0004】

また、この種のネットワークアクセスゲートウェイは、WAN側ネットワークインターフェースにWAN接続用IPアドレス／ネットマスク、デフォルトゲートウェイIPアドレスを設定し、さらにWANアクセスに必要なルーティングテーブルを設定することにより、LAN内のノードをWANに対してアクセスさせることが可能になる。ネットワークアクセスゲートウェイがLAN内の各ノードからのDNS(Domain Name System)クエリを中継処理するDNSプロキシ機能を持つ場合は、WANにおけるDNSサーバのIPアドレスの設定を行うこともある。DHCPクライアント機能を有するネットワークアクセスゲートウェイの場合は、上記のWAN側ネットワークインターフェースにおける設定およびルーティングテーブル、DNSクエリ転送テーブルにおける各設定パラメータをWAN内のDHCPサーバから払い出されることにより、自動的に行うことも可能である。この

10

20

30

40

50

他にも、WANへのアクセスが、WAN内の認証サーバに対してアクセス認証を行うことによって可能になる場合は、WANアクセスに必要な設定パラメータが上記認証サーバから払い出される場合もある。ネットワークアクセスゲートウェイと認証サーバとの間で用いられるプロトコルとしては、RADIUSプロトコルなどがある。

【0005】

WANアクセスに必要な各設定は、LAN内ノードからWANへのアクセスにおいて、LAN内の全てのノードによって共有される。例えば、ネットワークアクセスゲートウェイを介してWAN側に送信される全てのパケットは、WAN接続用IPアドレスにソースIPアドレスが変換されて送信される。また、WAN側にLAN内ノードからのアクセスの候補となる仮想的または物理的に分離された網（以下ターゲット網と呼ぶ）が複数存在する場合であっても、LAN内の各ノードからアクセスすることが可能なターゲット網は、ネットワークアクセスゲートウェイがアクセス認証されたターゲット網だけである。

10

【0006】

上述したネットワークアクセスゲートウェイは、LANとWANとの間で流れるパケットに対してレイヤ3レベル（IPレベル）の処理を行うものであった。さらにレイヤ2レベル（イーサネットレベル：イーサネットは登録商標）の処理を行う装置まで対象を広げると、従来から用いられている認証VLANスイッチも、ネットワークアクセスのためにLAN内ノードを収容する装置として挙げるができる。認証VLANスイッチは、配下のノードを認証によりアクセスが許可されたVLANへ接続するための機能を有するものである。

20

【特許文献1】特許第3153173号

【発明の開示】

【発明が解決しようとする課題】

【0007】

従来技術の第1の問題点は、ネットワークアクセスゲートウェイにおいて、LAN内の全てのノードは、WANへのアクセスのための環境設定を共有しなければならない点である。

【0008】

先にも述べたように、WANへのアクセスのための環境設定はLAN内の全てのノードで共有されるため、ネットワークアクセスゲートウェイを介してWAN側に送信される全てのパケットは、同一のWAN接続用IPアドレスにソースIPアドレスが変換されて送信される。そのため、WAN側ではLAN内の個別のノードをソースIPアドレスによって識別することはできないし、WAN側からLAN内の特定のノードを指定して通信を開始することはできない。

30

【0009】

また、WAN側にアクセスの候補となるターゲット網が複数存在する場合に、LAN内のノードごとに異なるターゲット網に対してアクセスさせたい場合であっても、アクセスするターゲット網の設定をLAN内のノードごとに変えることはできない。

【0010】

上述した認証VLANスイッチを用いる場合は、ノードごとに認証ベースで異なるVLAN（ターゲット網）へアクセスさせることができるが、認証VLANスイッチではレイヤ2レベルのパケット処理しか行えず、IPパケットの転送やIPアドレス変換の設定、DNSメッセージの転送設定など、レイヤ3レベル以上の処理を行うことはできない。例えば、1台のノードが2つ以上のターゲット網に同時にアクセスしようとする場合、レイヤ2レベルの処理ではノードからのパケットをどのターゲット網に転送すればよいか識別することができず、限界がある。すなわち、認証VLANスイッチを用いる方法では、LAN内ノードは1つのターゲット網にしかアクセスすることはできない。

40

【0011】

従来技術の第2の問題点は、従来技術の第1の問題点が解決され、LAN内のノードごとにWANへのアクセスのための環境設定を変えることができるようになったとしても、

50

L A N内のノードは、I Pアドレス領域の重複する複数のターゲット網にアクセスすることができない点である。

【0012】

例えば、1台のL A N内のノードが、ターゲット網Xとターゲット網Yの2つのターゲット網へのアクセスが許可されたとする。このときもしもターゲット網Xとターゲット網Yの両方で10/8というI Pアドレス領域が用いられる場合、上記ノードから上記I Pアドレス領域に含まれる宛先へのI Pパケットは、ネットワークアクセスゲートウェイにおいてどちらのターゲット網に転送すべきか判断できない。すなわち、従来技術においては、I Pアドレス領域の重複する複数のターゲット網にアクセスすることは不可能である。

10

【0013】

〔発明の目的〕

本発明の第1の目的は、L A N内のノードごとにターゲット網に対する異なるアクセス環境を提供し、これにより、各ノードが任意の数のターゲット網に同時にアクセス可能な環境を提供できるネットワークアクセスゲートウェイを提供することである。

【0014】

本発明の第2の目的は、L A N内のノードがI Pアドレス領域の重複する複数のターゲット網にアクセスすることを可能とするネットワークアクセスゲートウェイを提供することにある。

【課題を解決するための手段】

20

【0015】

本発明にかかる第1のネットワークアクセスゲートウェイは、L A N内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにするため、

L A Nと該L A N内のノードからのアクセスの候補となる複数のターゲット網を含むW A Nとの境界に設置され、前記L A N内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、

前記ノードごとに、1つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えることを特徴とする。

【0016】

本発明にかかる第2のネットワークアクセスゲートウェイは、ターゲット網への不正なアクセスを防ぐため、第1のネットワークアクセスゲートウェイにおいて、

30

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする。

【0017】

本発明にかかる第3のネットワークアクセスゲートウェイは、L A N内のノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにすると共に、ターゲット網への不正なアクセスを防ぐため、

L A Nと該L A N内のノードからのアクセスの候補となる複数のターゲット網を含むW A Nとの境界に設置され、前記L A N内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、

40

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部と、

該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部とを備えることを特徴とする。

【0018】

本発明にかかる第4のネットワークアクセスゲートウェイは、第3のネットワークアクセスゲートウェイにおいて、

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノード

50

がアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする。

【0019】

本発明にかかる第5のネットワークアクセスゲートウェイは、第3または第4のネットワークアクセスゲートウェイにおいて、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第2のエントリが格納される名前解決クエリ転送テーブルとを備え、

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記ルーティングテーブルに対して第1のエントリを作成し、前記名前解決クエリ転送テーブルに対して第2のエントリを作成することを特徴とする。

【0020】

本発明にかかる第6のネットワークアクセスゲートウェイは、第5のネットワークアクセスゲートウェイにおいて、

前記名前解決クエリはDNSクエリであり、前記名前解決クエリ転送テーブルはDNSクエリ転送テーブルであることを特徴とする。

【0021】

本発明にかかる第7のネットワークアクセスゲートウェイは、端末認証部の構成を簡単なものとするため、第3～第6の何れかのネットワークアクセスゲートウェイにおいて、

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする。

【0022】

本発明にかかる第8のネットワークアクセスゲートウェイは、端末認証部の構成を簡単なものにするため、第3～第6の何れかのネットワークアクセスゲートウェイにおいて、

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証VLANスイッチに問い合わせることにより認証を行うことを特徴とする。

【0023】

本発明にかかる第9のネットワークアクセスゲートウェイは、セッション管理部の構成を簡単なものにするため、第3～第8の何れかのネットワークアクセスゲートウェイにおいて、

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントを有することを特徴とする。

【0024】

本発明にかかる第10のネットワークアクセスゲートウェイは、アドレス詐称等によるなりすましを防ぐため、第3～第9の何れかのネットワークアクセスゲートウェイにおいて、

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられることを特徴とする。

【0025】

本発明にかかる第11のネットワークアクセスゲートウェイは、LAN内のノードがIPアドレス領域の重複する複数のターゲット網にアクセスできるようにするため、第3～

10

20

30

40

50

第10のネットワークアクセスゲートウェイの何れかにおいて、

複数の前記ターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求める機能を有するIPアドレス領域重複検出部を備えることを特徴とする。

【0026】

本発明にかかる第12のネットワークアクセスゲートウェイは、第11のネットワークアクセスゲートウェイにおいて、

前記セッション管理部は、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記IPアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第3のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するIPアドレス領域を互いに重複しないIPアドレス領域にIPアドレス変換するように第1のエントリおよび第3のエントリを設定することを特徴とする。

【0027】

本発明にかかる第13のネットワークアクセスゲートウェイは、第12のネットワークアクセスゲートウェイにおいて、

前記名前解決クエリはDNSクエリであり、前記名前解決応答はDNS応答であり、前記名前解決クエリ／応答転送テーブルはDNSクエリ／応答転送テーブルであることを特徴とする。

【0028】

本発明にかかる第1のネットワークアクセスゲートウェイの制御方法は、ネットワークアクセスゲートウェイに収容されているLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにするため、

LANと該LAN内のノードからのアクセスの候補となる複数のターゲット網を含むWANとの境界に設置され、前記LAN内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、

前記ノードごとに、1つまたは複数の前記ターゲット網へのアクセスのための環境設定を行うことを特徴とする。

【0029】

本発明にかかる第2のネットワークアクセスゲートウェイの制御方法は、ターゲット網への不正なアクセスを防ぐため、第1のネットワークアクセスゲートウェイの制御方法において、

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする。

【0030】

本発明にかかる第3のネットワークアクセスゲートウェイの制御方法は、LAN内のノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにすると共に、ターゲット網への不正なアクセスを防止するため、

LANと該LAN内のノードからのアクセスの候補となる複数のターゲット網を含むWANとの境界に設置され、前記LAN内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証

10

20

30

40

50

ステップと、

該端末認証ステップで認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理ステップとを含むことを特徴とする。

【0031】

本発明にかかる第4のネットワークアクセスゲートウェイの制御方法は、第3のネットワークアクセスゲートウェイの制御方法において、

前記セッション管理ステップは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする。

10

【0032】

本発明にかかる第5のネットワークアクセスゲートウェイの制御方法は、第3または第4のネットワークアクセスゲートウェイの制御方法において、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第2のエントリが格納される名前解決クエリ転送テーブルとを備え、

前記セッション管理ステップでは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

20

前記ルーティングテーブルに対して第1のエントリを作成し、前記名前解決クエリ転送テーブルに対して第2のエントリを作成することを特徴とする。

【0033】

本発明にかかる第6のネットワークアクセスゲートウェイの制御方法は、第5のネットワークアクセスゲートウェイの制御方法において、

前記名前解決クエリはDNSクエリであり、前記名前解決クエリ転送テーブルはDNSクエリ転送テーブルであることを特徴とする。

【0034】

本発明にかかる第7のネットワークアクセスゲートウェイの制御方法は、端末認証ステップにおける処理を簡単なものとするため、第3～第6の何れかのネットワークアクセスゲートウェイの制御方法において、

30

前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする。

【0035】

本発明にかかる第8のネットワークアクセスゲートウェイの制御方法は、端末認証ステップの処理を簡単なものとするため、第3～第6の何れかのネットワークアクセスゲートウェイの制御方法において、

40

前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証VLANスイッチに問い合わせることにより認証を行うことを特徴とする。

【0036】

本発明にかかる第9のネットワークアクセスゲートウェイの制御方法は、セッション管理部の構成を簡単なものにするため、第3～第8の何れかのネットワークアクセスゲートウェイの制御方法において、

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのため

50

の環境設定に必要なパラメータの一部または全てを取得するパラメータ取得ステップを含むことを特徴とする。

【0037】

本発明にかかる第10のネットワークアクセスゲートウェイの制御方法は、アドレス詐称等によるなりすましを防ぐため、第3～第9の何れかのネットワークアクセスゲートウェイの制御方法において、

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられることを特徴とする。

【0038】

本発明にかかる第11のネットワークアクセスゲートウェイの制御方法は、LAN内のノードがIPアドレス領域の重複する複数のターゲット網にアクセスできるようにするため、第3～第10のネットワークアクセスゲートウェイの制御方法の何れかにおいて、

複数の前記ターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求める機能を有するIPアドレス領域重複検出ステップを含むことを特徴とする。

【0039】

本発明にかかる第12のネットワークアクセスゲートウェイの制御方法は、第11のネットワークアクセスゲートウェイの制御方法において、

前記セッション管理ステップでは、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記IPアドレス領域重複検出ステップを介して、前記複数のターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第3のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するIPアドレス領域を互いに重複しないIPアドレス領域にIPアドレス変換するように第1のエントリおよび第3のエントリを設定することを特徴とする。

【0040】

本発明にかかる第13のネットワークアクセスゲートウェイの制御方法は、第12のネットワークアクセスゲートウェイの制御方法において、

前記名前解決クエリはDNSクエリであり、前記名前解決応答はDNS応答であり、前記名前解決クエリ／応答転送テーブルはDNSクエリ／応答転送テーブルであることを特徴とする。

【0041】

本発明にかかる第1のプログラムは、ネットワークアクセスゲートウェイに收容されるLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにするため、

コンピュータを、LANと該LAN内のノードからのアクセスの候補となる複数のターゲット網を含むWANとの境界に設置され、前記LAN内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、前記ノードごとに、1つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えるネットワークアクセスゲートウェイとして機能させることを特徴とする。

【0042】

本発明にかかる第2のプログラムは、ターゲット網への不正なアクセスを防ぐため、第1のプログラムにおいて、

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする。

【0043】

本発明にかかる第3のプログラムは、ネットワークアクセスゲートウェイに收容されるLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにすると共に、ターゲット網への不正なアクセスを防止するため、

コンピュータを、LANと該LAN内のノードからのアクセスの候補となる複数のターゲット網を含むWANとの境界に設置され、前記LAN内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部、

該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部として機能させることを特徴とする。

【0044】

本発明にかかる第4のプログラムは、第3のプログラムにおいて、

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする。

【0045】

本発明にかかる第5のプログラムは、第3または第4のプログラムにおいて、

前記コンピュータが、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第2のエントリが格納される名前解決クエリ転送テーブルとを備え、

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記ルーティングテーブルに対して第1のエントリを作成し、前記名前解決クエリ転送テーブルに対して第2のエントリを作成することを特徴とする。

【0046】

本発明にかかる第6のプログラムは、第5のプログラムにおいて、

前記名前解決クエリはDNSクエリであり、前記名前解決クエリ転送テーブルはDNSクエリ転送テーブルであることを特徴とする。

【0047】

本発明にかかる第7のプログラムは、端末認証部における処理を簡単なものとするため、第3～第6の何れかのプログラムにおいて、

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする。

【0048】

本発明にかかる第8のプログラムは、端末認証部の処理を簡単なものとするため、第3～第6の何れかのプログラムにおいて、

10

20

30

40

50

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証VLANスイッチに問い合わせることにより認証を行うことを特徴とする。

【0049】

本発明にかかる第9のプログラムは、セッション管理部の構成を簡単なものにするため、第3～第8の何れかのプログラムにおいて、

前記コンピュータを、

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントとして機能させることを特徴とする。

10

【0050】

本発明にかかる第10のプログラムは、アドレス詐称等によるなりすましを防ぐため、第3～第9の何れかのプログラムにおいて、

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられることを特徴とする。

【0051】

本発明にかかる第11のプログラムは、LAN内のノードがIPアドレス領域の重複する複数のターゲット網にアクセスできるようにするため、第3～第10のプログラムの何れかにおいて、

20

前記コンピュータを、

複数の前記ターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求めるIPアドレス領域重複検出部として機能させることを特徴とする。

【0052】

本発明にかかる第12のプログラムは、第11のプログラムにおいて、

前記セッション管理部は、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記IPアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求め、

30

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第1のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第3のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するIPアドレス領域を互いに重複しないIPアドレス領域にIPアドレス変換するように第1のエントリおよび第3のエントリを設定することを特徴とする。

40

【0053】

本発明にかかる第13のプログラムは、第12のプログラムにおいて、

前記名前解決クエリはDNSクエリであり、前記名前解決応答はDNS応答であり、前記名前解決クエリ／応答転送テーブルはDNSクエリ／応答転送テーブルであることを特徴とする。

【発明の効果】

【0054】

本発明にかかる第1のネットワークアクセスゲートウェイによれば、ネットワークアクセスゲートウェイに收容されているLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。

50

【0055】

その理由は、ネットワークアクセスゲートウェイが、ノード毎に、1つまたは複数のターゲット網へのアクセスのための環境設定を行う構成を備えているからである。

【0056】

本発明にかかる第2のネットワークアクセスゲートウェイは、ターゲット網への不正なアクセスを防ぐことができるという効果を有する。

【0057】

その理由は、認証が成功したことを契機として環境設定を行うようにしているからである。

【0058】

本発明にかかる第3のネットワークアクセスゲートウェイによれば、ネットワークアクセスゲートウェイに收容されているLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができると共に、ターゲット網に対する不正アクセスを防止できるという効果を得ることができる。

【0059】

その理由は、複数のターゲット網に対してノードがアクセスするための認証を行う端末認証部と、認証が成功したアクセスのための環境設定を行うセッション管理部とを備えているからである。

【0060】

本発明にかかる第4のネットワークアクセスゲートウェイは、第3のネットワークアクセスゲートウェイと同様の効果を有する。

【0061】

その理由は、セッション管理部が、端末認証部によってアクセスすることを許可されたターゲット網に対してノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成する構成を有しているからである。

【0062】

本発明にかかる第5のネットワークアクセスゲートウェイは、第3のネットワークアクセスゲートウェイと同様の効果を有する。

【0063】

その理由は、セッション管理部が、端末認証部によってアクセスすることが許可されたターゲット網とノードとの間でパケットを送受信するための第1のエントリをルーティングテーブル上に作成すると共に、端末認証部によってアクセスすることを許可されたターゲットに対して名前解決クエリを転送するための第2のエントリを名前解決クエリ転送テーブル上に作成するからである。

【0064】

本発明にかかる第6のネットワークアクセスゲートウェイは、第3のネットワークアクセスゲートウェイと同様の効果を有する。

【0065】

その理由は、名前解決クエリがDNSクエリであり、名前解決クエリ転送テーブルがDNSクエリ転送テーブルであるからである。

【0066】

本発明にかかる第7のネットワークアクセスゲートウェイは、認証機能がターゲット網内の認証サーバに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

【0067】

その理由は、ターゲット網内に存在する認証サーバに対して問い合わせを行うことにより、認証を行うようにしているからである。

【0068】

本発明にかかる第8のネットワークアクセスゲートウェイは、認証機能が認証VLANスイッチに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効

10

20

30

40

50

果を有する。

【0069】

その理由は、認証VLANスイッチに対して問い合わせを行うことにより、認証を行っているからである。

【0070】

本発明にかかる第9のネットワークアクセスゲートウェイは、環境設定に必要なパラメータが設定サーバに保持されているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

【0071】

その理由は、設定サーバから環境設定に必要なパラメータの一部または全てを取得する設定クライアントを備えているからである。

10

【0072】

本発明にかかる第10のネットワークアクセスゲートウェイは、アドレス詐称等によるなりすましを防ぐことができるという効果を有する。

【0073】

その理由は、ノードとの接続において、ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクを用いるからである。

【0074】

本発明にかかる第11のネットワークアクセスゲートウェイは、ネットワークアクセスゲートウェイに収容されているLAN内のノードが、IPアドレス領域の重複する複数のターゲット網にアクセスできるという効果を有する。

20

【0075】

その理由は、複数の前記ターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求めるIPアドレス領域重複検出部を備えているからである。

【0076】

本発明にかかる第12のネットワークアクセスゲートウェイは、第11のネットワークアクセスゲートウェイと同様の効果を有する。

【0077】

その理由は、LAN内のノードからの認証要求に基づいて上記ノードが所望するターゲット網へのアクセスが可能になるように設定を行う際に、上記ノードに対してアクセスが許可されたターゲット網間にIPアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないIPアドレス領域にIPアドレス変換すべく、ルーティングテーブルエントリ、名前解決クエリ／応答転送テーブルエントリの設定を行うからである。

30

【0078】

本発明にかかる第13のネットワークアクセスゲートウェイは、第11のネットワークアクセスゲートウェイと同様の効果を有する。

【0079】

その理由は、名前解決クエリがDNSクエリであり、名前解決応答がDNS応答であり、名前解決クエリ／応答転送テーブルがDNSクエリ／応答転送テーブルであるからである。

40

【0080】

本発明にかかる第1のネットワークアクセスゲートウェイの制御方法によれば、ネットワークアクセスゲートウェイに収容されるLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。

【0081】

その理由は、ネットワークアクセスゲートウェイが、ノード毎に、1つまたは複数のターゲット網へのアクセスのための環境設定を行うからである。

50

本発明にかかる第２のネットワークアクセスゲートウェイの制御方法は、ターゲット網への不正なアクセスを防ぐことができるという効果を有する。

その理由は、認証が成功したことを契機として環境設定を行うようにしているからである。

本発明にかかる第3のネットワークアクセスゲートウェイの制御方法によれば、ネットワークアクセスゲートウェイに收容されているLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。共に、ターゲット網に対する不正アクセスを防止できるという効果を得ることができる。

その理由は、複数のターゲット網に対してノードがアクセスするための認証を行う端末認証ステップと、認証が成功したアクセスのための環境設定を行うセッション管理ステップとを含んでいるからである。

本発明にかかる第４のネットワークアクセスゲートウェイの制御方法は、第３のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。

その理由は、セッション管理ステップにおいて、端末認証ステップによってアクセスすることを許可されたターゲット網に対してノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成するようにしているからである。

本発明にかかる第 5 のネットワークアクセスゲートウェイの制御方法は、第 3 のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。

その理由は、セッション管理ステップにおいて、アクセスすることが許可されたターゲット網とノードとの間でパケットを送受信するための第1のエントリをルーティングテーブル上に作成する処理と、アクセスすることを許可されたターゲットに対して名前解決クエリを転送するための第2のエントリを名前解決クリエ転送テーブル上に作成する処理を行うからである。

本発明にかかる第 6 のネットワークアクセスゲートウェイの制御方法は、第 3 のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。

その理由は、名前解決クエリがDNSクエリであり、名前解決クエリ転送テーブルがDNSクエリ転送テーブルであるからである。

本発明にかかる第7のネットワークアクセスゲートウェイの制御方法は、認証機能がターゲット網内の認証サーバに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

その理由は、ターゲット網内に存在する認証サーバに対して問い合わせを行うことにより、認証を行うようにしているからである。

本発明にかかる第 8 のネットワークアクセスゲートウェイの制御方法は、認証機能が認証 V L A N スイッチに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

その理由は、認証 VLAN スイッチに問い合わせることにより認証を行うからである。

【0096】

本発明にかかる第9のネットワークアクセスゲートウェイの制御方法は、環境設定に必要なパラメータが設定サーバに保持されているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

【0097】

その理由は、設定サーバから環境設定に必要なパラメータの一部または全てを取得するパラメータ取得ステップを含んでいるからである。

【0098】

本発明にかかる第10のネットワークアクセスゲートウェイの制御方法は、アドレス詐称等によるなりすましを防ぐことができるという効果を有する。

10

【0099】

その理由は、ノードとの接続において、ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクを用いるからである。

【0100】

本発明にかかる第11のネットワークアクセスゲートウェイの制御方法は、ネットワークアクセスゲートウェイに收容されているLAN内のノードが、IPアドレス領域の重複する複数のターゲット網にアクセスできるという効果を有する。

【0101】

その理由は、複数の前記ターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求めるIPアドレス領域重複検出ステップを含んでいるからである。

20

【0102】

本発明にかかる第12のネットワークアクセスゲートウェイの制御方法は、第11のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。

【0103】

その理由は、LAN内のノードからの認証要求に基づいて、上記ノードが所望するターゲット網へのアクセスが可能になるように設定を行う際に、上記ノードに対してアクセスが許可されたターゲット網間にIPアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないIPアドレス領域にIPアドレス変換すべく、ルーティングテーブルエントリ、名前解決クエリ／応答転送テーブルエントリの設定を行うからである。

30

【0104】

本発明にかかる第13のネットワークアクセスゲートウェイの制御方法は、第11のネットワークアクセスゲートウェイと同様の効果を有する。

【0105】

その理由は、名前解決クエリがDNSクエリであり、名前解決応答がDNS応答であり、名前解決クエリ／応答転送テーブルがDNSクエリ／応答転送テーブルであるからである。

【0106】

本発明にかかる第1のプログラムによれば、ネットワークアクセスゲートウェイに收容に收容されるLAN内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。

40

【0107】

その理由は、コンピュータを、ノード毎に、1つまたは複数のターゲット網へのアクセスのための環境設定を行うネットワークアクセスゲートウェイとして機能させるからである。

【0108】

本発明にかかる第2のプログラムは、ターゲット網への不正なアクセスを防ぐことができるという効果を有する。

50

その理由は、認証が成功したことを契機として環境設定を行うようにしているからである。

【 0 1 1 1 】

10

本発明にかかる第 4 のプログラムは、第 3 のプログラムと同様の効果を有する。

その理由は、セッション管理部において、端末認証部によってアクセスすることを許可されたターゲット網に対してノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成するようにしているからである。

本発明にかかる第5のプログラムは、第3のプログラムと同様の効果を有する。

その理由は、セッション管理部が、アクセスすることが許可されたターゲット網とノードとの間でパケットを送受信するための第1のエントリをルーティングテーブル上に作成すると共に、アクセスすることを許可されたターゲットに対して名前解決クエリを転送するための第2のエントリを名前解決クエリ転送テーブル上に作成するからである。

本発明にかかる第 6 のプログラムは、第 3 のプログラムと同様の効果を有する。

その理由は、名前解決クエリがDNSクエリであり、名前解決クエリ転送テーブルがDNSクエリ転送テーブルであるからである。

本発明にかかる第7のプログラムは、認証機能がターゲット網内の認証サーバに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

その理由は、ターゲット網内に存在する認証サーバに対して問い合わせを行うことにより、認証を行うようにしているからである

本発明にかかる第 8 のプログラムは、認証機能が認証 V L A N スイッチに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

その理由は、認証 V L A N スイッチに問い合わせることにより認証を行うからである。

本発明にかかる第9のプログラムは、環境設定に必要なパラメータが設定サーバに保持されているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

その理由は、コンピュータ上に、設定サーバから環境設定に必要なパラメータの一部または全てを取得する設定クライアントを実現するようにしているからである。

本発明にかかる第 10 のプログラムは、アドレス詐称等によるなりすましを防ぐことができるという効果を有する。

【0125】

その理由は、ノードとの接続において、ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクを用いるからである。

【0126】

本発明にかかる第11のプログラムは、ネットワークアクセスゲートウェイに收容されているLAN内のノードが、IPアドレス領域の重複する複数のターゲット網にアクセスできるという効果を有する。

【0127】

その理由は、コンピュータ上に、複数のターゲット網の各々で利用されているIPアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するIPアドレス領域をどのようにIPアドレス変換すべきかを求めるIPアドレス領域重複検出部を実現するからである。

10

【0128】

本発明にかかる第12のプログラムは、第11のプログラムと同様の効果を有する。

【0129】

その理由は、LAN内のノードからの認証要求に基づいて、上記ノードが所望するターゲット網へのアクセスが可能になるように設定を行う際に、上記ノードに対してアクセスが許可されたターゲット網間にIPアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないIPアドレス領域にIPアドレス変換すべく、ルーティングテーブルエントリ、名前解決クエリ/応答転送テーブルエントリの設定を行うからである。

20

【0130】

本発明にかかる第13のプログラムは、第11のプログラムと同様の効果を有する。

【0131】

その理由は、名前解決クエリがDNSクエリであり、名前解決応答がDNS応答であり、名前解決クエリ/応答転送テーブルがDNSクエリ/応答転送テーブルであるからである。

【発明を実施するための最良の形態】

【0132】

次に本発明の実施の形態について図面を参照して詳細に説明する。

30

【0133】

図1を参照すると、本発明の第1の実施の形態は、端末A1とネットワークアクセスゲートウェイB1とスイッチングハブC1とターゲットVLAN D1～D3とによって実現される。ここで、ターゲット網は、以下で詳しく述べるイーサネットのVLANによって分離されているものとして説明するが、その他の方法（例えばIPsec、L2TP、MPLS (MultiProtocol Label Switching)等のトンネル技術によるVPNなど）で仮想的または物理的に分離された網であってもよいものとする。

【0134】

端末A1は、ターゲットVLAN D1～D3に含まれる1つ以上のネットワークに対してアクセスを行うLAN内のノードであり、PC (Personal Computer)、携帯端末、ワークステーション、IP電話機などが例に挙げられる。他にも、背景技術で示したような、配下に端末が接続されているネットワークアクセスゲートウェイも、ターゲットVLAN D1～D3に含まれる1つ以上のネットワークに対してアクセスを行うLAN内のノードとして挙げるができるが、以下、このようなノードも含めて端末A1として説明する。

40

【0135】

端末A1は、ネットワークアクセスゲートウェイB1の配下のLANに属する端末の1つである。端末A1のIPアドレスは、手動で設定されてもよいし、ネットワークアクセスゲートウェイB1または他のサーバの提供するDHCP (Dynamic Host Configuration Protocol)機能を用いて取得してもよい。端末A1は、ターゲットVLAN D1～D3に

50

含まれるネットワークへは通常アクセスすることはできず、アクセスしたい際は、ネットワークアクセスゲートウェイB1に対して所望のターゲットVLANへのアクセスに対する認証要求を行う。このアクセス認証要求に対応するターゲットVLANの数は1つでもよいし、複数であってもよい。認証の結果、アクセスが許可されると、アクセスが許可されたターゲットVLANへのアクセスを行うことが可能になる。ネットワークアクセスゲートウェイB1に対して認証要求を行う方法の例として、端末A1がネットワークアクセスゲートウェイB1の表示するWeb認証画面に、アクセスしたいターゲットVLANにおけるユーザIDおよびパスワードを入力する方法などが挙げられる。

【0136】

ネットワークアクセスゲートウェイB1は、端末A1をはじめとするLAN内の端末とWAN側のネットワークであるターゲットVLAN D1～D3とを接続する機能を有するアクセスゲートウェイであり、認証ベースでLAN内の端末ごとに異なるネットワークアクセス環境を提供する機能を有する。ネットワークアクセスゲートウェイB1は、その内部構成として、端末認証部B11とセッション管理部B12とルーティングテーブルB13とルーティング処理部B14とDNSクエリ転送テーブルB15とDNSプロキシ部B16とインターフェースドライバB17とネットワークインターフェースB18とを含む。

【0137】

スイッチングハブC1は、ネットワークアクセスゲートウェイB1に対して複数のターゲットVLANが収容できるようにするためにネットワークアクセスゲートウェイB1とターゲットVLAN D1～D3との間に設置される。このようにネットワークアクセスゲートウェイB1から同一リンク上に複数のネットワークセグメントを収容できるようにするために、イーサネットにおけるVLAN機能（IEEE 802.1qで定義されている）が利用される。VLAN機能を使った場合、ネットワークアクセスゲートウェイB1とターゲットVLAN D1～D3との間の通信は、スイッチングハブC1やネットワークアクセスゲートウェイB1においてVLANタグの値を見ることにより、どのターゲットVLANに対応するパケットであるかを識別可能となる。

【0138】

ターゲットVLAN D1～D3は、端末A1がアクセスを行うターゲットとなるネットワーク（ターゲット網）である。図1に示した例では、3つのターゲットVLANが記載されているが、任意の数のターゲットVLANが存在してよい。端末A1はネットワークアクセスゲートウェイB1に認証要求を出し、所望のターゲットVLANに対するアクセス認証を行う。アクセスが許可されると、ターゲットVLAN内およびこのターゲットVLANを経由してアクセス可能な網内のWebサーバ、メールサーバ等の各種サーバ、またはその他の端末と通信することにより、通信サービスを受けることができる。以下、簡単のために、ターゲットVLANを経由してアクセス可能な網も含めてターゲットVLANとよぶ。

【0139】

次にネットワークアクセスゲートウェイB1の構成について以下に詳細に記す。

【0140】

端末認証部B11は、端末A1がネットワークアクセスゲートウェイB1に対して行う認証要求を処理し、その結果、端末A1から所望のターゲットVLANへのアクセスが可能であると判断した場合、セッション管理部B12に対して端末A1から所望のターゲットVLANへのアクセスを行うために必要な設定を行うよう指示し、さらに端末A1に対して、アクセスが許可された旨を通知する。また、認証の結果、アクセスが不可能であると判断した場合は、端末A1に対してアクセスが許可されなかった旨を通知する。

【0141】

セッション管理部B12に対して端末A1から所望のターゲットVLANへのアクセスを行うために必要な設定を行うよう指示する場合、設定に必要なパラメータを端末認証部B11からセッション管理部B12に対して渡す。このために必要なパラメータは、端末

10

20

30

40

50

認証部 B 1 1 に予め登録されていてもよいし、あるいはこのパラメータを保持する外部のサーバから取得してもよい。設定に必要なパラメータを外部サーバから取得する場合は、端末認証部 B 1 1 はパラメータを取得する機能を有する。

【 0 1 4 2 】

セッション管理部 B 1 2 は、端末 A 1 をはじめとする LAN 内端末からのターゲット V LAN へのアクセスが認証により許可されると、端末ごとに異なるネットワークアクセス環境が提供できるようにルーティングテーブル B 1 3、DNS クエリ転送テーブル B 1 5、インターフェースドライバ B 1 7 に対して必要な設定を行う機能を有する。以下に具体的な設定内容を記す。

【 0 1 4 3 】

本実施の形態においては、端末ごとに異なるネットワークアクセス環境が提供できるように、ターゲット V LAN へのアクセスが許可された端末ごとに、アクセスが許可されたターゲット V LAN 数分だけのインターフェースが割り当てられる。そこで、認証により端末からターゲット V LAN へのアクセスが許可されると、セッション管理部 B 1 2 は、インターフェースドライバ B 1 7 へ指示を出し、アクセスが許可されたターゲット V LAN に対応する仮想インターフェースを作成する。具体的には、作成する仮想インターフェースの識別子 (eth0:1 など)、MAC アドレス、接続用 IP アドレス/ネットマスクを設定する。V LAN タグの使用によってターゲット V LAN が仮想的に区切られている場合は、アクセスするターゲット V LAN に対応する V LAN タグ ID も同時に設定する。

【 0 1 4 4 】

次にルーティングテーブル B 1 3 に対し、アクセスが許可されたターゲット V LAN へのルーティングテーブルエントリを設定する。具体的には、ターゲット V LAN ごとに、端末からの入力インターフェース、端末の IP アドレス (ソース IP アドレス)、ターゲット V LAN へアクセスするときの接続用 IP アドレス (宛先 IP アドレス)、ターゲット V LAN の IP アドレス領域 (ソース IP アドレス)、ターゲット V LAN におけるゲートウェイ IP アドレス及びターゲット V LAN への出力インターフェースを設定する。更に、ターゲット V LAN 毎に、ターゲット V LAN からの入力インターフェース、ターゲット V LAN の IP アドレス領域 (ソース IP アドレス)、端末へアクセスするときの接続用 IP アドレス (宛先 IP アドレス)、端末の IP アドレス (宛先 IP アドレス)、端末への出力インターフェースを設定する。

【 0 1 4 5 】

さらに、DNS クエリ転送テーブル B 1 5 に対し、端末からの DNS クエリをターゲット V LAN へ転送するためのエントリを設定する。具体的には、端末からの入力インターフェース、端末の IP アドレス、ターゲット V LAN に対応するドメインネーム領域および IP アドレス領域、ターゲット V LAN における DNS サーバの IP アドレス、ターゲット V LAN への出力インターフェースを設定する。

【 0 1 4 6 】

ルーティングテーブル B 1 3 は、ルーティング処理部 B 1 4 が行うパケットの転送処理のルールが記述されているテーブルである。ルーティングテーブル B 1 3 の設定は、セッション管理部 B 1 2 によってなされることが可能である。図 2 にルーティングテーブル B 1 3 の例を示す。図 2 を参照すると、入力されたパケットに対して、このパケットを出力するための方法が登録されている。例えば、インターフェース eth1 から入力し、ソース IP アドレスが 192.168.0.2 であるパケットに対しては、宛先 IP アドレスに応じて出力方法が異なり、宛先 IP アドレスが先頭ビットに 8 ビットのマスクをかけると 10.0.0.0 になる場合 (10/8 は先頭 8 ビットにマスクをかけると 10.0.0.0 となる IP アドレス群のことを示す。すなわち 10.1.2.3 や 10.2.3.4 などが当てはまる。)、ソース IP アドレスを 10.1.1.1 に書き換え、インターフェース eth0:0 から出力する。この場合のゲートウェイの IP アドレスは 10.1.1.254 である。また、宛先 IP アドレスが先頭ビットに 8 ビットのマスクをかける

10

20

30

40

50

と20.0.0.0になる場合は、ソースIPアドレスを20.1.1.1に書き換え、インターフェースeth0:1から出力する。この場合のゲートウェイのIPアドレスは20.1.1.254である。別のエントリでは、インターフェースeth0:0から入力した、10/8のIPアドレス領域に含まれるソースIPアドレス、10.1.1.1の宛先IPアドレスをもつパケットは、宛先IPアドレスを192.168.0.2に書き換え、インターフェースeth1から出力することが示されている。なお、図2において、eth1は、端末A1側の物理インターフェースを表し、eth0:0~eth0:4は、ターゲットVLAN側の物理インターフェースeth0上に作成された仮想インターフェースを表している。

【0147】

ここで、ルーティングテーブルB13における入力パケットの識別方法として、インターフェース識別子、ソースIPアドレス、宛先IPアドレスの他に、ソースMACアドレスなどのパケットに含まれる他のフィールドの情報を用いてもよい。また、IPsecやL2TPやMPLSなどの仮想リンクをエミュレートするトンネリングプロトコルを用いている場合は、仮想リンクに対応する仮想インターフェースの識別子を用いることも可能である。

【0148】

ルーティング処理部B14は、ネットワークアクセスゲートウェイB1が受信したパケットを、ルーティングテーブルB13に登録されているパケット転送ルールにしたがって転送を行う機能を有する。

【0149】

DNSクエリ転送テーブルB15は、端末A1が送信したDNSクエリをDNSプロキシ部B16がどのように転送するかを示すルールが登録されており、セッション管理部B12によって設定されることが可能である。DNSクエリ転送テーブルB15の例を図3に示す。図3を参照すると、インターフェースeth1から入力し、ソースIPアドレスが192.168.0.2であるDNSクエリに対しては、クエリ内容に応じてDNSクエリの転送方法が異なり、aaa.comドメインに含まれるドメインネーム(www.aaa.comやftp.xxx.aaa.comなど)に対応するIPアドレスを解決するDNSクエリおよび10/8のIPアドレスプレフィックスに含まれるIPアドレスに対応するドメインネームを解決するDNSクエリの場合は、ソースIPアドレスを10.1.1.1とし、出力インターフェースeth0:0から、10.1.2.3に対応するDNSサーバへDNSクエリを転送し、bbb.comドメインに含まれるドメインネームに対応するIPアドレスを解決するDNSクエリおよび20/8のIPアドレスプレフィックスに含まれるIPアドレスに対応するドメインネームを解決するDNSクエリの場合は、ソースIPアドレスを20.1.1.1とし、出力インターフェースeth0:1から、20.1.2.3に対応するDNSサーバへDNSクエリを転送するというルールが示されている。

【0150】

ここで、DNSクエリ転送テーブルB15における入力DNSクエリの識別方法として、インターフェース識別子、ソースIPアドレス、入力クエリ内容の他に、ソースMACアドレスなどのパケットに含まれる他のフィールドの情報を用いてもよい。また、IPsecやL2TPやMPLSなどの仮想リンクをエミュレートするトンネリングプロトコルを用いている場合は、仮想リンクに対応する仮想インターフェースの識別子を用いることも可能である。

【0151】

DNSプロキシ部B16は、端末A1が送信したDNSクエリを一旦受信し、DNSクエリ転送テーブルB15に登録されているルールにしたがって、上記DNSクエリを送信した端末A1を識別してさらに送信した端末A1およびクエリ内容(すなわちクエリに含まれるドメインネームまたはIPアドレス)に基づいてターゲットVLAN内のDNSサーバに対して上記DNSクエリを転送する。さらにターゲットVLAN内のDNSサーバ

10

20

30

40

50

から受信したDNS応答を、DNSクエリを送信した端末A1に対して転送する。

【0152】

インターフェースドライバB17は、ネットワークアクセスゲートウェイB1のもつネットワークインターフェースB18を制御するドライバモジュールであり、データリンクレイヤレベルの packets 送受信処理を行う。インターフェースドライバB17は、ネットワークインターフェースB18内に複数の仮想的なインターフェースを作成する機能を有し、この機能により、物理的なネットワークインターフェース上に任意の数の仮想インターフェースを持たせることができる。また、各仮想インターフェースごとにMACアドレス、VLANタグID、IPアドレス、ネットマスクの設定を行うことができる。図4に物理的なネットワークインターフェース上に複数の仮想インターフェースが設定される例をインターフェース設定テーブル103として示す。図4を参照すると、eth0で示される物理インターフェース上に、eth0:0, eth0:1, eth0:2, eth0:3, eth0:4で示される5つの仮想インターフェースが設定されており、それぞれに異なるMACアドレス、VLANタグID、IPアドレス、ネットマスクが設定されている。仮想インターフェースの設定は、セッション管理部B12によってなされることが可能である。

10

【0153】

ここで、インターフェースドライバB17でもつことの可能な仮想インターフェースは、MACアドレスまたはVLANタグIDで区別できる仮想インターフェースだけではなく、IPsecやL2TPやMPLSなどの仮想リンクをエミュレートするトンネリングプロトコルの仮想リンクのインターフェースであってもよい。例えば、図4の例では、LAN側のインターフェースはeth1の1つしかないが、LAN内の各端末に対して個別にIPsecトンネルが作成される場合は、各端末に対応する仮想リンクのインターフェースがLAN側の仮想インターフェースとして設定される。あるいは、ターゲット網がMPLSのラベルによって仮想的に分離されている場合は、WAN側の仮想インターフェースとしてMPLSのインターフェースが用いられる。このようなトンネリングプロトコルを用いる効果としては、アドレス詐称等によるなりすましを防ぎ、ネットワークアクセスゲートウェイB1において、接続されている端末A1を確実に一意に識別できるようになることが挙げられる。

20

【0154】

次に、図5を参照して、本実施の形態において、端末A1がネットワークアクセスゲートウェイB1に対して、WAN内のターゲットVLANへアクセスするための認証要求を出した場合のネットワークアクセスゲートウェイB1における動作について詳細に説明する。

30

【0155】

ここでは、端末A1はターゲットVLAN D1とターゲットVLAN D2の2つのターゲットVLANに対してアクセスするための認証要求を出すものとする。ターゲットVLAN D1およびD2の識別子は、それぞれaaa.com、bbb.comであり、ドメインネーム領域、IPアドレス領域はそれぞれaaa.com、10/8およびbbb.com、20/8であるとする。また、ターゲットVLAN D1とターゲットVLAN D2はそれぞれVLANタグIDが100、200のVLANでスイッチングハブC1によって論理的に分割されているものとする。端末A1は、ネットワークアクセスゲートウェイB1のインターフェースeth1の配下に存在し、192.168.0.2のIPアドレスをもつものとする。

40

【0156】

端末A1がWAN内のターゲットVLANへアクセスするための認証要求をネットワークアクセスゲートウェイB1へ送信すると、端末認証部B11がこの認証要求を受信する。この認証要求には、端末A1がアクセスしようとしているターゲットVLANを示す識別子と、認証のために必要なパラメータ(ID、パスワードなど)が含まれており、認証要求に含まれるパラメータに基づいてユーザがアクセス可能であるかどうかの認証を行う

50

(図5のステップS101)。例えば認証要求に、[taro@aaa.com/pass-1][taro@bbb.com/pass-2]というメッセージが埋め込まれている場合は、aaa.comに対応するドメイン(ターゲットVLAN D1)に対してtaro/pass-1というユーザID/パスワードで、bbb.comに対応するドメイン(ターゲットVLAN D2)に対してtaro/pass-2というユーザID/パスワードでアクセス認証を行いたいということを示すものである。ここでは、各ターゲットVLANごとにユーザID/パスワードが必要となる例について示したが、他にも、1つのユーザID/パスワードで複数のターゲットVLANに対するアクセス認証を行う方法も可能である。

【0157】

ステップS101におけるアクセス認証の結果、端末A1から所望するターゲットVLANへのアクセスを許可できると判断された場合(ステップS102がイエス)、端末認証部B11は、セッション管理部B12に対して、アクセスが許可されたターゲットVLANへのアクセスに必要な設定を行うよう指示する(ステップS103)。このとき、端末A1に対応する入力インターフェース(eth1)、IPアドレス(192.168.0.2)とともに、アクセスが許可されたターゲットVLANの識別子(aaa.comとbbb.com)、およびそれぞれのターゲットVLANに対するVLANタグID(100と200)、接続用IPアドレス/ネットマスク(10.1.1.1/255.255.255.0と20.1.1.1/255.255.255.0)、ゲートウェイIPアドレス(10.1.1.254と20.1.1.254)、ドメインネーム領域(aaa.comとbbb.com)、IPアドレス領域(10/8と20/8)、DNSサーバIPアドレス(10.1.2.3と20.1.2.3)が設定に必要なパラメータとして渡される。上記カッコ内に記載されたパラメータは、本実施の形態において渡される実際のパラメータの例である。以下、上記カッコ内に記載されたパラメータが渡されたものとして説明を行う。

【0158】

ステップS103の結果、セッション管理部B12はまず、アクセスが許可されたターゲットVLANに対応する仮想インターフェースを作成するようにインターフェースドライバB17に対して指示を出す(ステップS104)。ここでは、ターゲットVLAN D1へのアクセスのために図4におけるeth0:0のエントリで示される仮想インターフェースが作成され、ターゲットVLAN D2へのアクセスのためにeth0:1のエントリで示される仮想インターフェースが作成される。

【0159】

ステップS104の次に、セッション管理部B12は、アクセスが許可されたターゲットVLANへ端末A1からのパケットを転送するためのルーティングテーブルエントリをルーティングテーブルB13に対して作成する(ステップS105)。ここでは、図2の入力ソースIPアドレスが192.168.0.2に対応するエントリが作成される。このエントリには、アクセスが許可された各ターゲットVLANに対応して、ターゲットVLAN D1宛のパケット(宛先IPアドレスが10/8の場合)のルーティング方法と、ターゲットVLAN D2宛のパケット(宛先IPアドレスが20/8の場合)のルーティング方法がそれぞれ登録されている。更に、ここでは、図2のインターフェースeth0:0及びインターフェースeth0:1に対応するエントリも作成される。インターフェースeth0:0に対応するエントリには、ターゲットVLAN D1から端末A1へのパケットのルーティング方法が登録され、インターフェースeth0:1に対応するエントリには、ターゲットVLAN D2から端末A1へのパケットのルーティング方法が登録されている。

【0160】

ステップS105の次に、セッション管理部B12は、端末A1が送信したDNSクエリを転送するためのエントリをDNSクエリ転送テーブルB15に対して設定する(ステップS106)。ここでは、図3の入力ソースIPアドレスが192.168.0.2に

10

20

30

40

50

対応するエントリが作成される。アクセスが許可された各ターゲットVLANに対応して、ターゲットVLAN D1へのDNSクエリ（ドメインネーム領域がaaa.com、IPアドレス領域が10/8である場合）の転送方法と、ターゲットVLAN D2へのDNSクエリ（ドメインネーム領域がaaa.com、IPアドレス領域が10/8である場合）の転送方法がそれぞれ登録されている。

【0161】

ステップS106の後、セッション管理部B12は、端末認証部B11に対して指示された設定が終了したことを通知し、端末認証部B11は、アクセス認証成功を伝えるメッセージを端末A1に対して応答する（ステップS107）。このメッセージが応答されると、端末A1は認証により許可されたターゲットVLANへのアクセスを行うことが可能となる。

10

【0162】

また、ステップS101におけるアクセス認証の結果、端末A1から所望するターゲットVLANへのアクセスを許可できないと判断された場合、端末認証部B11は、アクセス認証失敗を伝えるメッセージを端末A1に対して応答する（ステップS108）。

【0163】

以上、本実施の形態におけるネットワークアクセスゲートウェイB1における動作について説明した。

【0164】

以下、本実施の形態から考えられる他の実施の形態についても併せて説明する。

20

【0165】

1つ目は、端末認証部B11が端末A1からの認証要求に対して直接認証を行うのではなく、各ターゲットVLAN D1～D3に存在する認証サーバE1～E3に対して認証要求を転送し、認証サーバE1～E3が実際の認証を行う形態である（図6を参照）。

【0166】

この場合、端末認証部B11は、端末A1から受信した認証要求を解析し、端末A1がアクセスしたいターゲットVLANに対応する認証サーバへ上記認証要求を転送する。例えば端末認証部B11が端末A1から受信した認証要求に、[taro@aaa.com/pass-1] [taro@bbb.com/pass-2]というメッセージが埋め込まれている場合は、aaa.comに対応するターゲットVLAN内の認証サーバへは、[taro/pass-1]の部分を送信し、bbb.comに対応するターゲットVLAN内の認証サーバへは、[taro/pass-2]の部分を送信するという動作を端末認証部B11が行う。セッション管理部B12が行う設定に必要なパラメータは、端末認証部B11が認証サーバE1～E3から取得する。

30

【0167】

2つ目は、ネットワークアクセスゲートウェイB1が認証VLANスイッチC2によってターゲットVLAN D1～D3と接続されており、端末認証部B11が端末A1からの認証要求に対して直接認証を行うのではなく、認証VLANスイッチC2に対して認証要求を送信し、認証VLANスイッチC2（もしくは認証VLANスイッチに接続されている外部の認証サーバ；この外部の認証サーバは多段構成になっていてもよい）が実際の認証を行う形態である（図7を参照）。このような認証VLANスイッチC2の例として、IEEE802.1xに対応した認証VLANスイッチが挙げられる。

40

【0168】

この場合、端末認証部B11は、端末A1から受信した認証要求を認証VLANスイッチC2に対して送信する。IEEE802.1xに対応した認証VLANスイッチが用いられる場合は、認証メッセージを送受信するプロトコルとして、EAPOL(Extensible Authentication Protocol Over Lans)が用いられるため、端末A1と端末認証部B11との間で送受信するためのプロトコルはEAPOL形式に変換される。端末A1が2つ以上のターゲットVLANへの認証要求を送信している場合は、端末認証部B11は認証を要求されている各ターゲットVLAN D1～D3ごとに対応するEAPOLフレームを認

50

証VLANスイッチC2に対して送信する。

【0169】

3つ目は、端末A1から所望のターゲットVLANへのアクセスを行うために必要な全ての設定パラメータを端末認証部B11からセッション管理部B12へ渡すのではなく、一部のパラメータを、ターゲットVLAN内の設定サーバから、ネットワークアクセスゲートウェイが備える設定クライアントが自動的に取得して設定を行う形態である。この種の設定サーバ、設定クライアントとしては、それぞれDHCPサーバ、DHCPクライアントが一般的に用いられる。他にも、IPv6で用いられるNDP(Neighbor Discovery Protocol)機能を用いる方法もある。以下、DHCPサーバ、DHCPクライアントが用いられる場合を例に挙げて説明する。

10

【0170】

この場合、図8に示すように、各ターゲットVLAN D1～D3内にはDHCPサーバ(DHCPサーバF1～F3)が存在し、さらにネットワークアクセスゲートウェイB1の代わりに、DHCPクライアントB19を有するネットワークアクセスゲートウェイB2が用いられる。DHCPクライアントB19は、DHCPサーバF1～F3からターゲットVLAN D1～D3へのアクセスに必要なパラメータを取得し、取得したパラメータをセッション管理部B12に渡す。セッション管理部B12は、渡された設定パラメータを用いて、インターフェースドライバB17、ルーティングテーブルB13、DNSクエリ転送テーブルB15に対して設定を行う。

【0171】

20

さらにこの場合のネットワークアクセスゲートウェイB2の動作を図9に示す。ステップ104において、ターゲットVLANごとに仮想インターフェースを作成した後、アクセスが許可された各ターゲットVLAN内のDHCPサーバから設定パラメータを取得して(ステップS109)から、セッション管理部B12が上記仮想インターフェースにおけるIPアドレス/ネットマスクの設定(ステップS110)、ルーティングテーブルエントリの作成(ステップS105)、DNSクエリ転送テーブルの作成(ステップS106)を行う点が、先に図5で示したネットワークアクセスゲートウェイB1の動作と異なる。ここで、ステップS104の時点では、作成された仮想インターフェースに対してIPアドレス/ネットマスクは設定されていないことに注意する。

【0172】

30

DHCPサーバから取得できるパラメータは、接続用IPアドレス/ネットマスク、デフォルトゲートウェイIPアドレス、IPアドレス領域が主なものである。その他、MACアドレスなど、設定に必要なパラメータでDHCPサーバから取得することができないものに関しては、端末認証部B11から渡される。

【0173】

4つ目は、ネットワークアクセスゲートウェイB1において、DNSプロトコルにおけるクエリ/応答だけではなく、その他の種類の名前解決プロトコルにおけるクエリ/応答のプロキシ処理が行われる形態である。その他の種類の名前解決プロトコルとして、LDAP(Lightweight Directory Access Protocol)やWINS(Windows Internet Name Service: Windowsは登録商標)プロトコルなどが挙げられる。この場合は、本実施の形態におけるDNSクエリ転送テーブルB15およびDNSプロキシ部B16の代わりあるいは追加として、名前解決クエリ転送テーブルおよび名前解決プロキシ部が用いられ、名前解決クエリ転送テーブルおよび名前解決プロキシ部がその他の種類の名前解決プロトコルに対するプロキシ処理を行う。

40

【0174】

なお、図1、図6、図7に示したネットワークアクセスゲートウェイB1や、図8に示したネットワークアクセスゲートウェイB2はコンピュータによって実現可能である。ネットワークアクセスゲートウェイB1をコンピュータによって実現する場合には、コンピュータをネットワークアクセスゲートウェイB1として機能させるためのプログラムを記録した記録媒体(ディスク、半導体メモリ、その他の記録媒体)を用意しておく。コンピ

50

ュータは、この記録媒体に記録されたプログラムを読み込み、自身の動作を制御することにより、自コンピュータ上に、端末認証部B11、セッション管理部B12、ルーティングテーブルB13、ルーティング処理部B14、DNSクエリ転送テーブルB15、DNSプロシキ部B16、インターフェースドライバB17、ネットワークインターフェースB18を実現する。また、ネットワークアクセスゲートウェイB2をコンピュータによって実現する場合には、コンピュータをネットワークアクセスゲートウェイB2として機能させるためのプログラムを記録した記録媒体（ディスク、半導体メモリ、その他の記録媒体）を用意しておく。コンピュータは、この記録媒体に記録されたプログラムを読み込み、自身の動作を制御することにより、自コンピュータ上に、端末認証部B11、セッション管理部B12、ルーティングテーブルB13、ルーティング処理部B14、DNSクエリ転送テーブルB15、DNSプロシキ部B16、インターフェースドライバB17、ネットワークインターフェースB18、DHCPクライアントB19を実現する。

10

【0175】

次に本実施の形態の効果について説明する。

【0176】

本実施の形態では、ネットワークアクセスゲートウェイB1は、LAN内の端末A1からの認証要求に基づき、端末A1が所望するターゲットVLANへのアクセスが可能になるように、インターフェースドライバB17に対して仮想インターフェースを作成するとともに、端末A1が送受信するパケットを転送するための設定をルーティングテーブルB13に対して行い、さらに端末A1が送信するDNSクエリを転送するための設定をDNSクエリ転送テーブルB15に対して行う。

20

【0177】

従来技術では、ネットワークアクセスゲートウェイにおけるWAN側のインターフェースは、LAN内の全ての端末に対して共有される。すなわち、LAN内の全ての端末に対して同一のWAN側の設定が用いられねばならなかった。本実施の形態により、LAN内端末からの認証に基づいて、この端末のWANアクセスのために個別の仮想インターフェース、ルーティングテーブルエントリ、DNSクエリ転送テーブルエントリが作成されるため、LAN内の端末ごとに異なるターゲット網に対するアクセス環境を提供することが可能になる。また、仮想インターフェース、ルーティングテーブルエントリ、DNSクエリ転送テーブルエントリの設定は、端末に対してアクセスが許可された任意の数のターゲット網に対して行われるため、端末に対して任意の数のターゲット網に同時にアクセス可能な環境を提供することが可能となる。

30

【0178】

次に、本発明の第2の実施の形態について図面を参照して詳細に説明する。

【0179】

図10を参照すると、本発明の第2の実施の形態は、ネットワークアクセスゲートウェイB1の代わりに、ネットワークアクセスゲートウェイB3が用いられる点が図1に示した本発明の第1の実施の形態における構成と異なる。ネットワークアクセスゲートウェイB3は、DNSクエリ転送テーブルB15の代わりにDNSクエリ／応答転送テーブルB21を有する点、ルーティングテーブルB13の代わりにルーティングテーブルB13aを有する点、およびIPアドレス領域重複検出部B20を有する点でネットワークアクセスゲートウェイB1の構成と異なる。

40

【0180】

セッション管理部B12は、本実施の第1の実施の形態で説明した機能に加えて、端末A1に対して複数のターゲットVLANへのアクセスが許可された場合に、IPアドレス領域重複検出部B20に問い合わせて各ターゲットVLANに対応するIPアドレス領域に重複があるかないかを調べる。重複があった場合、ターゲットVLAN内のDNSサーバからのDNS応答を、重複しないIPアドレスに変換して端末A1に転送するよう、DNSクエリ／応答変換テーブルB21に対して設定する。さらに、ルーティングテーブルB13aに対しても、DNSクエリ／応答のIPアドレス変換に対応してルーティング処

50

理部 B 1 4 が I P アドレス変換を行うようにエントリを設定する。

【 0 1 8 1 】

I P アドレス領域重複検出部 B 2 0 は、セッション管理部 B 1 2 からの要求に基づいて、各ターゲット V L A N に対応する I P アドレス領域について I P アドレス領域の重複があるかを調べて応答する。さらに、重複を検出した場合は、各ターゲット V L A N の I P アドレス領域が重複しないためにはどのように I P アドレス変換すべきかを求め、セッション管理部 B 1 2 に対して応答する。

【 0 1 8 2 】

図 1 1 に I P アドレス領域重複検出部 B 2 0 の動作の例を示す。1 つ目の例では、セッション管理部 B 1 2 が、ターゲット V L A N D 1 (I P アドレス領域 : 1 0 / 8) とターゲット V L A N D 2 (I P アドレス領域 : 2 0 / 8) の 2 つのターゲット V L A N について I P アドレス領域が重複するかどうかを検出する要求を送った場合、2 つの I P アドレス領域には重複がないため、I P アドレス領域重複検出部 B 2 0 は、重複なしを応答する。2 つ目の例では、セッション管理部 B 1 2 が、ターゲット V L A N D 1 (I P アドレス領域 : 1 0 / 8) とターゲット V L A N D 3 (I P アドレス領域 : 1 0 / 8) の 2 つのターゲット V L A N について I P アドレス領域が重複するかどうかを検出する要求を送った場合、2 つの I P アドレス領域は重複するため、I P アドレス領域重複検出部 B 2 0 は、ターゲット V L A N D 3 については、1 0 / 8 の I P アドレスを 3 0 / 8 に I P アドレス変換すれば重複しないという応答をする。なお、この応答内容はあくまで一例であり、重複しない I P アドレス領域を応答するものであれば、どのようなものであっても良い。

【 0 1 8 3 】

D N S クエリ / 応答転送テーブル B 2 1 は、D N S クエリ転送テーブル B 1 5 に設定されるパラメータに加えて、D N S プロキシ部 B 1 6 がターゲット V L A N 内の D N S サーバからの D N S 応答を端末 A 1 に転送する際に、応答する I P アドレスをどのように変換すべきかというパラメータがエントリとして格納されているテーブルである。図 1 2 に D N S クエリ / 応答転送テーブル B 2 1 の例を示す。図 1 2 を参照すると、I P アドレス変換が必要なターゲット V L A N に対する D N S クエリ / 応答に関しては、D N S クエリ / 応答転送用のパラメータとして実際の I P アドレス領域と変換する I P アドレス領域が設定される。ドメインネーム領域が a a a . c o m であるターゲット V L A N に関しては D N S クエリ / 応答に対して I P アドレス変換を行う必要はないが、ドメインネーム領域が c c c . c o m であるターゲット V L A N に対しては、実際のターゲット V L A N の I P アドレス領域が 1 0 / 8 であるものを、3 0 / 8 の I P アドレス領域に D N S プロキシ部 B 1 6 で変換して L A N 内端末にみせる必要があることを示す。この場合の D N S プロキシ部 B 1 6 における D N S クエリおよび D N S 応答の変換の例を図 1 3 に示す。ここで、D N S サーバ G 1 は、ドメインネーム領域が c c c . c o m であるターゲット V L A N 内にある D N S サーバである。

【 0 1 8 4 】

図 1 3 を参照すると、A レコード解決と P T R レコード解決との 2 種類の D N S メッセージの変換の例が示されている。A レコード解決 (ドメインネームに対する I P アドレスの解決。I P v 6 の場合は A A A A レコードを解決する。) の場合、D N S プロキシ部 B 1 6 は、端末 A 1 から受信した D N S クエリについてはそのままターゲット V L A N 内の D N S サーバ G 1 に転送するが、D N S サーバ G 1 から戻された D N S 応答については、w w w . c c c . c o m に対応する I P アドレスを 1 0 . 2 . 3 . 4 から 3 0 . 2 . 3 . 4 に変換して端末 A 1 に転送している。また、P T R レコード解決 (I P アドレスに対するドメインネームの解決) の場合、D N S プロキシ部 B 1 6 は、端末 A 1 から受信した D N S クエリについては、3 0 . 2 . 3 . 4 を 1 0 . 2 . 3 . 4 に変換して D N S サーバ G 1 に転送し、D N S サーバ G 1 から戻された D N S 応答については、そのまま端末 A 1 に転送している。すなわちターゲット V L A N 側では実際には 1 0 / 8 の I P アドレス領域が用いられているが、端末 A 1 には上記ターゲット V L A N 側においてあたかも 3 0 / 8

のIPアドレス領域が用いられていると見せるようにDNSプロキシ部B16によってDNSメッセージのIPアドレスを変換する。

【0185】

次に、DNSプロキシ部B16が行うDNSクエリ／応答のIPアドレス変換に対応して、ルーティング処理部B14もIPアドレス変換を行うように、セッション管理部B12がルーティングテーブルB13aに対して行う設定について説明する。

【0186】

図12に示したDNSクエリ／応答転送テーブルB21に対応するルーティングテーブルB13aの例を図14に示す。図14を参照すると、第1番目のエントリでは、端末A1から受信したパケット（入力インターフェース：eth1，ソースIPアドレス：192.168.0.5）に対して、10/8のIPアドレス領域に含まれる宛先IPアドレスの場合は、ソースIPアドレスを10.1.1.3に変換してeth0:5のインターフェースから出力するのに対し、30/8のIPアドレス領域に含まれる宛先IPアドレスの場合は、ソースIPアドレスを10.1.1.3に変換し、宛先IPアドレスを10/8のIPアドレス領域のIPアドレスに変換してから、eth0:6のインターフェースから出力するというを示している。ここで、30/8の宛先IPアドレスを10/8のIPアドレス領域に変換するというのは、30.3.4.5を10.3.4.5に変換するというように、30/8の領域に含まれるIPアドレスを10/8の領域に含まれるIPアドレスに1対1にマッピングすることを示している。

【0187】

ルーティングテーブルB13aの第2番目と第3番目のエントリは、ターゲットVLANから受信したパケットに対するルーティング方法が登録されている。第2番目のエントリでは、eth0:5の仮想インターフェースから入力した、ソースIPアドレスが10/8のIPアドレス領域に含まれ、宛先IPアドレスが10.1.1.3であるパケットに対しては、宛先IPアドレスを192.168.0.5に変換して、eth1のインターフェースから出力するというを示している。第3番目のエントリでは、eth0:6の仮想インターフェースから入力した、ソースIPアドレスが10/8のIPアドレス領域に含まれ、宛先IPアドレスが10.1.1.3であるパケットに対しては、宛先IPアドレスを192.168.0.5に変換すると共にソースIPアドレスを30/8に変換してeth1のインターフェースから出力するというを示している。

【0188】

次に、図15を参照して、本実施の形態において、端末A1がネットワークアクセスゲートウェイB3に対して、WAN内のターゲットVLANへアクセスするための認証要求を出した場合のネットワークアクセスゲートウェイB3における動作について詳細に説明する。

【0189】

図15に示すステップS201～S208の動作はそれぞれ、図5に示した本発明の第1の実施の形態の動作における、ステップS101～S108に対応する。図15に示す動作は、ステップS204でアクセスが許可された各ターゲットVLANに対応する仮想インターフェースを作成してからステップS205でルーティングテーブルエントリの作成を行うまでの動作が異なる。

ステップS204の後、セッション管理部B12は、端末A1に対してアクセスが許可された各ターゲットVLANに対するIPアドレスをIPアドレス領域重複検出部B20に渡し、IPアドレス領域重複検出部B20はそれぞれのIPアドレス領域に重複がないかを調べる（ステップS210）。ここで、端末A1から新規にアクセスできるように設定しているターゲットVLAN間のIPアドレス領域重複だけではなく、既に端末A1に対してアクセスが許可されて設定が完了しているターゲットVLANとのIPアドレス領域重複も調べられる。

【0190】

ステップS210の結果、IPアドレス領域に重複がなければそのままステップS20

10

20

30

40

50

5に進む。

【0191】

ステップS210の結果、IPアドレス領域に重複があれば、IPアドレス領域重複検出部B20は、各ターゲットVLANのIPアドレス領域が重複しないためにはどのようにIPアドレス変換すべきかを求め、セッション管理部B12に対して応答する（ステップS211）。

【0192】

ステップS211の後、ステップS205およびS206で、セッション管理部B12はルーティングテーブルB13aおよびDNSクエリ／応答転送テーブルB21の設定を行うが、ここではステップS210で求められたIPアドレス変換方法がルーティングテーブルB13aおよびDNSクエリ／応答転送テーブルB21の設定に反映される。

10

【0193】

また、第1の実施の形態では、

1. 端末認証部B11が端末A1からの認証要求に対して直接認証を行うのではなく、各ターゲットVLANに存在する認証サーバE1～E3に対して認証要求を転送し、認証サーバE1～E3が実際の認証を行う形態
2. ネットワークアクセスゲートウェイB1が認証VLANスイッチC2によってターゲットVLAN D1～D3と接続されており、端末認証部B11が端末A1からの認証要求に対して直接認証を行うのではなく、認証VLANスイッチC2に対して認証要求を転送し、認証VLANスイッチC2（もしくは認証VLANスイッチに接続されている外部の認証サーバ）が実際の認証を行う形態
3. 端末A1から所望のターゲットVLANへのアクセスを行うために必要な全ての設定パラメータを、端末認証部B11からセッション管理部B12へ渡すのではなく、一部の設定パラメータを、ターゲットVLAN内の設定サーバからネットワークアクセスゲートウェイ内の設定クライアントが自動的に取得して設定を行う形態
4. ネットワークアクセスゲートウェイB1において、DNSプロトコルにおけるクエリ／応答だけでなく、その他の種類の名前解決プロトコルにおけるクエリ／応答のプロキシ処理が行われる形態

20

の4つの考えられる他の実施の形態についても併せて説明したが、第2の実施の形態においても、同様の実施の形態をとることが可能である。

30

【0194】

なお、図10に示したネットワークアクセスゲートウェイB3は、コンピュータによって実現可能である。ネットワークアクセスゲートウェイB3をコンピュータによって実現する場合には、コンピュータをネットワークアクセスゲートウェイB3として機能させるためのプログラムを記録した記録媒体（ディスク、半導体メモリ、その他の記録媒体）を用意しておく。コンピュータは、この記録媒体に記録されたプログラムを読み込み、自身の動作を制御することにより、自コンピュータ上に、端末認証部B11、セッション管理部B12、ルーティングテーブルB13a、ルーティング処理部B14、DNSプロキシ部B16、インターフェースドライバB17、ネットワークインターフェースB18、IPアドレス領域重複検出部B20、DNSクエリ応答転送テーブルB21を実現する。

40

【0195】

次に本実施の形態の効果について説明する。

【0196】

本実施の形態では、ネットワークアクセスゲートウェイB1は、LAN内の端末A1からの認証要求に基づいて端末A1が所望するターゲットVLANへのアクセスが可能になるように設定を行う際に、端末A1に対してアクセスが許可されたターゲットVLAN間にIPアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないIPアドレス領域にIPアドレス変換すべく、ルーティングテーブルB13のエントリ、DNSクエリ／応答転送テーブルB21のエントリの設定を行う。

【0197】

50

従来技術では、ネットワークアクセスゲートウェイは、LAN内端末を互いにIPアドレス領域が重複するターゲットVLANにアクセスさせることはできなかったが、本実施の形態により、端末の送受信するパケットおよびDNSクエリ／応答を互いに重複しないIPアドレス領域に変換することで、上記端末にはあたかも互いに重複しないIPアドレス領域をもつターゲットVLANにアクセスしているように見せることが可能になり、端末をIPアドレス領域の重複する複数のターゲットVLANにアクセスさせることが可能となる。

【図面の簡単な説明】

【0198】

【図1】本発明の第1の実施の形態の構成を示すブロック図である。

10

【図2】本発明の第1の実施の形態のルーティングテーブルの例を示す図である。

【図3】本発明の第1の実施の形態のDNSクエリ転送テーブルの例を示す図である。

【図4】本発明の第1の実施の形態のインターフェースドライバにおけるインターフェース設定テーブル例を示す図である。

【図5】本発明の第1の実施の形態のネットワークアクセスゲートウェイの動作を示すフローチャートである。

【図6】本発明の第1の実施の形態から考えられる1つ目の他の実施の形態の構成を示すブロック図である。

【図7】本発明の第1の実施の形態から考えられる2つ目の他の実施の形態の構成を示すブロック図である。

20

【図8】本発明の第1の実施の形態から考えられる3つ目の他の実施の形態の構成を示すブロック図である。

【図9】本発明の第1の実施の形態から考えられる3つ目の他の実施の形態のネットワークアクセスゲートウェイの動作を示すフローチャートである。

【図10】本発明の第2の実施の形態の構成を示すブロック図である。

【図11】本発明の第2の実施の形態のIPアドレス領域重複検出部の動作例を示すフローチャートである。

【図12】本発明の第2の実施の形態のDNSクエリ／応答転送テーブルの例を示す図である。

【図13】本発明の第2の実施の形態のDNSプロキシ部の動作例を示すフローチャートである。

30

【図14】本発明の第2の実施の形態のルーティングテーブルの例を示す図である。

【図15】本発明の第2の実施の形態のネットワークアクセスゲートウェイの動作を示すフローチャートである。

【符号の説明】

【0199】

A1…端末

B1～B3…ネットワークアクセスゲートウェイ

B11…端末認証部

B12…セッション管理部

40

B13、B13a…ルーティングテーブル

B14…ルーティング処理部

B15…DNSクエリ転送テーブル

B16…DNSプロキシ部

B17…インターフェースドライバ

B18…ネットワークインターフェース

B19…DHCPクライアント

B20…IPアドレス領域重複検出部

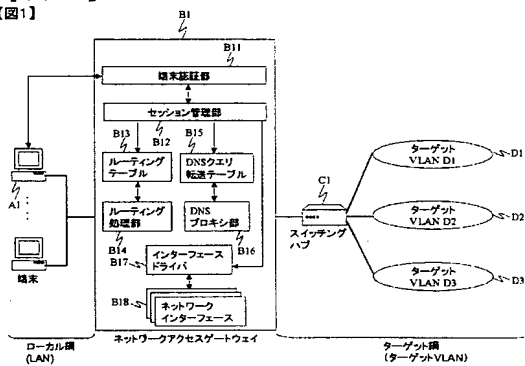
B21…DNSクエリ／応答転送テーブル

C1…スイッチングハブ

50

C 2 … 認証 VLAN スイッチ
 D 1 ～ D 3 … ターゲット VLAN
 E 1 ～ E 3 … 認証サーバ
 F 1 ～ F 3 … DHCP サーバ
 G 1 … DNS サーバ
 1 0 3 インターフェイス設定テーブル

【図 1】



【図 2】

103 ルーティングテーブル

入力 インターフェース	入力		出力			
	ソースIP アドレス	宛先IPアドレス	ソースIP アドレス	宛先IP アドレス	ゲートウェイ IPアドレス	出力 インターフェース
eth1	192.168.0.2	10/8	10.1.1.1	—	10.1.1.254	eth0.0
		20/8	20.1.1.1	—	20.1.1.254	eth0.1
	192.168.0.3	20/8	20.1.1.2	—	20.1.1.254	eth0.2
		10/8	10.1.1.2	—	10.1.1.254	eth0.3
192.168.0.4	10/8	10.1.1.2	—	10.1.1.254	eth0.4	
eth0.0	10/8	10.1.1.1	—	192.168.0.2	—	eth1
eth0.1	20/8	20.1.1.1	—	192.168.0.2	—	eth1
eth0.2	20/8	20.1.1.2	—	192.168.0.3	—	eth1
eth0.3	10/8	10.1.1.2	—	192.168.0.3	—	eth1
eth0.4	10/8	10.1.1.2	—	192.168.0.4	—	eth1

【図 3】

B15 DNSクエリ転送テーブル

入力 インターフェース	入力		出力	
	ソースIP アドレス	入力クエリ	ソースIP アドレス	出力 インターフェース
eth1	192.168.0.2	*.aaa.com, 10/8	10.1.1.1	10.1.2.3 eth0.0
		*.bbb.com, 20/8	20.1.1.1	20.1.2.3 eth0.1
	192.168.0.3	*.bbb.com, 20/8	20.1.1.2	20.1.2.3 eth0.2
		*.ccc.com, 10/8	10.1.1.2	10.1.3.4 eth0.3
	192.168.0.4	*.aaa.com, 10/8	10.1.1.2	10.1.2.3 eth0.4

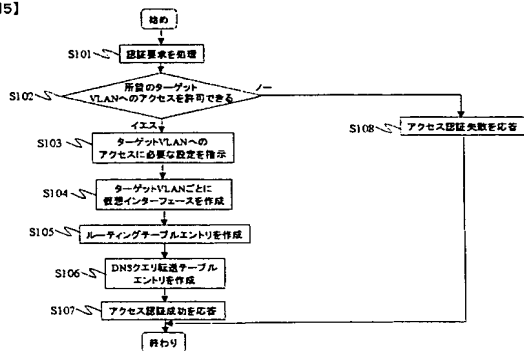
【図 4】

103 インターフェイス設定テーブル

物理 インターフェース	仮想 インターフェース	MACアドレス	VLANタグ ID	IPアドレス	ネットマスク
eth0	eth0.0	0.0.0.0.0.1	100	10.1.1.1	255.255.255.0
	eth0.1	0.0.0.0.0.2	200	20.1.1.1	255.255.255.0
	eth0.2	0.0.0.0.0.3	200	20.1.1.2	255.255.255.0
	eth0.3	0.0.0.0.0.4	300	10.1.1.1	255.255.255.0
	eth0.4	0.0.0.0.0.5	100	10.1.1.2	255.255.255.0
eth1	なし	1.2.3.4.5.6	なし	192.168.0.254	255.255.255.0
...

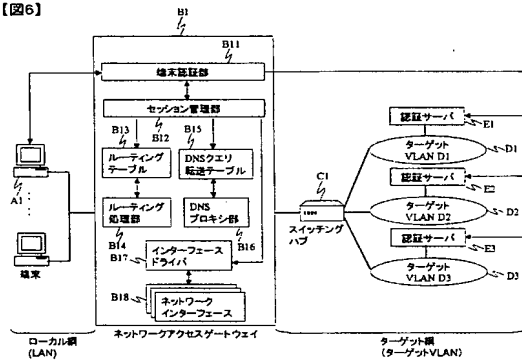
【図5】

【図5】



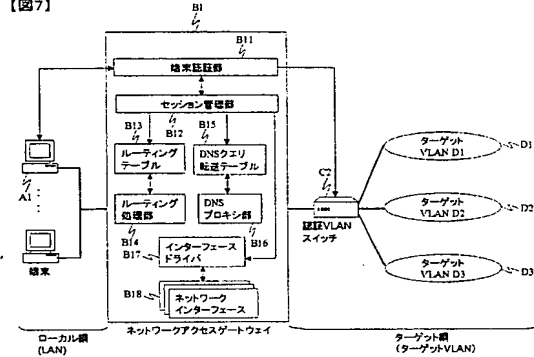
【図6】

【図6】



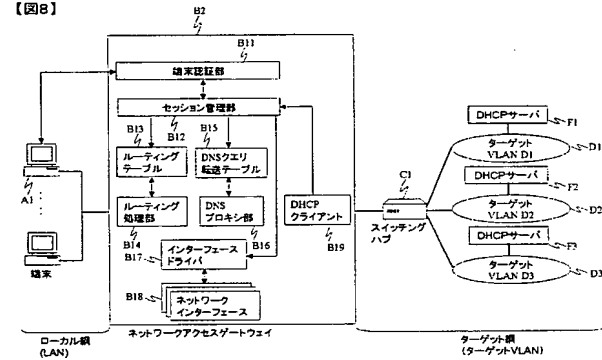
【図7】

【図7】



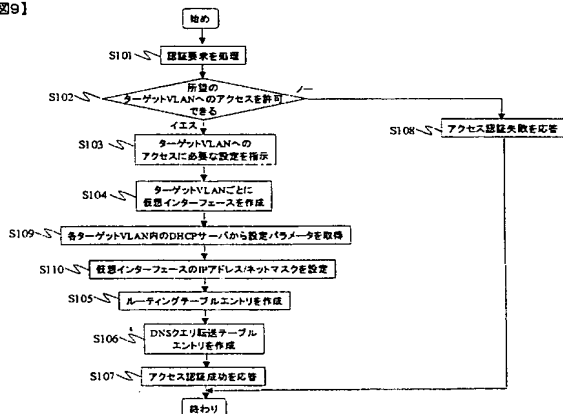
【図8】

【図8】



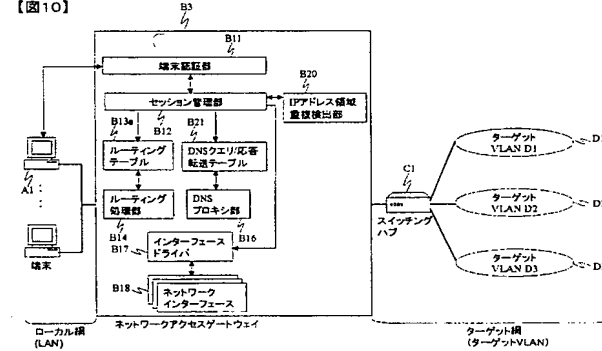
【図9】

【図9】



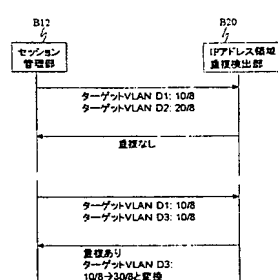
【図10】

【図10】



【図11】

【図11】



【図12】

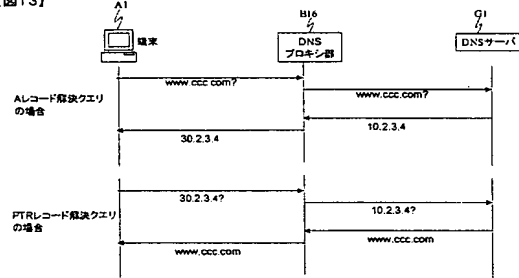
【図12】

B21 DNSクエリ応答転送テーブル

入力			出力			IPアドレス変換	
入力 インターフェース	ソースIP アドレス	入力クエリ	ソースIP アドレス	DNSサー バ	出力 インター フェース	宛先のIPア ドレス転送	宛先IPア ドレス転送
eth1	192.168.0.5	*.aaa.com, 10/8	10.1.1.3	10.1.2.3	eth0:5	—	—
		*.ccc.com, 30/8	10.1.1.3	10.1.3.4	eth0:6	10/8	30/8

【図13】

【図13】



【図14】

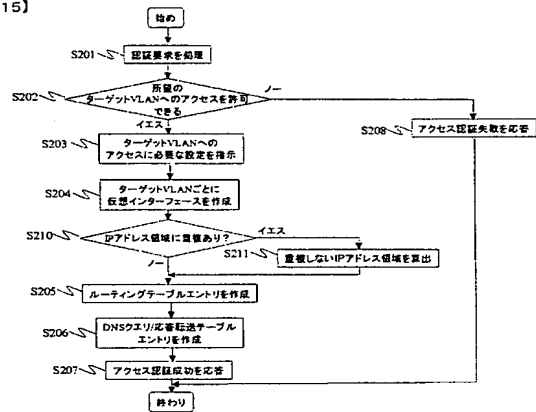
【図14】

B13a ルーティングテーブル

入力			出力		
入力 インターフェース	ソースIP アドレス	宛先IPアドレス	ソースIP アドレス	宛先IP アドレス	出力 インターフェース
eth1	192.168.0.5	10/8	10.1.1.3	—	eth0:5
		30/8	10.1.1.3	10/8	eth0:6
eth0:5	10/8	10.1.1.3	—	192.168.0.5	eth1
eth0:6	10/8	10.1.1.3	30/8	192.168.0.5	eth1

【図15】

【図15】



フロントページの続き

Fターム(参考) 5K030 HA08 HD03 HD06 HD09 KA01 KA05 LB01 LB06
5K033 CB09 CC01 DA06 DB12 DB18 EC04